In the Claims:

Please amend Claims 1, 7, 18, 24, 30, 35 and 36, all as shown below. Applicant reserves the right to prosecute any originally presented claims in a continuing or future application.

1. (Currently Amended) A security system for allowing a client to access a protected resource or application, said application including an application container, comprising:

an application interface mechanism for receiving ~~an access~~ a request from a client ~~application~~ to access a protected ~~resource~~ application, and communicating said ~~access~~ request to a security service, wherein the client makes the request on the application container, and the application container calls the security service with the request and a callback;

a security service for making a decision to permit or deny said ~~access~~ request, wherein the security service includes a plurality of security providers that may be plugged into the security service, and wherein the security providers use the callback handler to request context information from the application container for the request, and wherein depending on the output from the security providers the security service determines an entitlement for the client to use with the protected application; and[[,]]

a resource interface for communicating permitted access requests to said protected ~~resource~~ application.

2. (Original) The security system of claim 1 wherein said application interface mechanism includes an application container for reading an application deployment description and registering said deployment description within the security service.

3. (Original) The security system of claim 2 wherein said application container is an Enterprise Java Beans container.

4. (Original) The security system of claim 2 wherein said application container is a WebApp container.

5. (Original) The security system of claim 1 wherein said security service includes a plurality of access decision mechanisms for defining an access policy and for determining a contributory decision to permit, deny, or abstain from said access request.

6. (Original) The security system of claim 5 wherein said security service further includes an access controller for transferring said access request to said plurality of access decision mechanisms, and for combining said contributory decisions into an overall decision by the security service to permit or deny said access request.

7. (Currently Amended) The security system of claim 5 wherein said access ~~decisions~~ decision mechanisms represent a business function related access policy.

8. (Original) The security system of claim 5 wherein access decisions may be added to the security service to reflect changes in the access policy.

9. (Original) The security system of claim 5 wherein said access decision mechanisms are used to define an entitlement for said client to access said protected resource.

10. (Original) The security system of claim 5 wherein a deny or abstain by any one of said access decision mechanisms causes the security service to deny the access request.

11. (Original) The security system of claim 5 wherein an abstain by any one of said access decision mechanisms does not cause the security service to deny the access request.

12. (Original) The security system of claim 5 wherein said security service further includes an audit mechanism for auditing the determinations of said plurality of access requests.

13. (Original) The security system of claim 1 wherein said resource interface includes an interface mechanism to pass requests to or from a protected resource.

14. (Original) The security system of claim 13 wherein said interface mechanism includes a Java J2EE security interface.

15. (Original) The security system of claim 13 wherein said interface mechanism includes a security provider interface.

16. (Original) The security system of claim 13 wherein said interface mechanism is included as a plug-in in said resource interface.

17. (Original) The security system of claim 1 wherein the security service further makes a decision on whether to permit or deny a response to said access request from said protected resource to said client.

18. (Currently Amended) A method of allowing a client to access a protected ~~resource~~ application, said application including an application container, comprising:

receiving at an application container ~~interface mechanism an access~~ a request from a client ~~application~~ to access a protected ~~resource~~ application ~~and communicating said access request to a security service~~;

communicating the request from the application container to the security service together with a callback;

making a decision at said security service to permit or deny said access request, wherein the security service includes a plurality of security providers that may be plugged into the security service;

using the callback handler at each security provider to request context information from the application container for the request;

determining an entitlement for the client to use with the protected application depending on the output from the security providers; and[,]

communicating ~~via a resource interface~~ a permitted ~~access~~ request to ~~said~~ the protected ~~resource~~ application.

19. (Original) The method of claim 18 wherein said application interface mechanism includes an application container for reading an application deployment description and registering said deployment description within the security service.

20. (Original) The method of claim 19 wherein said application container is an Enterprise Java Beans container.

21. (Original) The method of claim 19 wherein said application container is a WebApp container.

22. (Original) The method of claim 18 further comprising:

defining an access policy via a plurality of access decision mechanisms within said security service; and,

determining at each access decision mechanism a contributory decision to permit, deny, or abstain from said access request.

23. (Original) The method of claim 22 further comprising:

transferring via an access controller said access request to said plurality of access decision mechanisms, and combining said contributory decisions into an overall decision by the security service to permit or deny said access request.

24. (Currently Amended) The method of claim 22 wherein said access ~~decisions~~ decision mechanisms represent a business function related access policy.

25. (Original) The method of claim 22 wherein access decisions may be added to the security service to reflect changes in the access policy.

26. (Original) The method of claim 22 further comprising:

using said access decision mechanisms to define an entitlement for said client to access said protected resource.

27. (Original) The method of claim 22 wherein a deny or abstain by any one of said access decision mechanisms causes the security service to deny the access request.

28. (Original) The method of claim 22 wherein an abstain by any one of said access decision mechanisms does not cause the security service to deny the access request.

29. (Original) The method of claim 22 further comprising:

auditing via an audit mechanism the determinations of said plurality of access requests.

30. (Currently Amended) The method of claim 18 wherein said step of communicating ~~via a resource interface~~ the request includes passing requests via an interface mechanism to or from a protected resource.

31. (Original) The method of claim 30 wherein said interface mechanism includes a Java J2EE security interface.

32. (Original) The method of claim 30 wherein said interface mechanism includes a security provider interface.

33. (Original) The method of claim 30 wherein said interface mechanism is included as a plug-in in said resource interface.

34. (Original) The method of claim 18 further comprising:

making a decision on whether to permit or deny a response to said access request from said protected resource to said client.

35. (Currently Amended) A method for determining a user entitlement to access protected resources in a secure environment, comprising:

receiving an access request from a user application to access a protected resource, by invoking a security service with said access request and a callback;

determining a user entitlement to access said protected resource, wherein said determining includes polling a plurality of security providers that may be plugged into the security service, and wherein the security providers use a callback handler to request context information from the application container for the request;

making a decision at said security service based on said user entitlement to permit or deny said access request; and[[,]]

the steps of either

(a) communicating a permitted access request to said protected resource, or

(b) denying a denied access request to said protected resource.

36. (Currently Amended) The method of claim 35 wherein if said request is permitted said entitlement also determines ~~the~~ a type of access available to the user of said protected resource.

37. (Original) The method of claim 36 wherein said type of access includes any of view, modify, delete, or copy, any part or all of said protected resource.

38. (Original) The method of claim 35 wherein information about said user entitlement can be communicated from a first security realm to a second security realm.

39. (Original) The method of claim 38 wherein additional information from a first security realm can be used to modify the user entitlement, prior to communicating said information about said user entitlement from said first security realm to said second security realm.